PATVIRTINTA
Asmens dokumentų išrašymo centro prie Lietuvos Respublikos vidaus reikalų ministerijos
direktoriaus 2019 m. spalio 28 d.
įsakymu Nr. 1-76

PILIEČIO SERTIFIKATO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Piliečio sertifikato taisyklės (toliau – taisyklės) nustato į Lietuvos Respublikos piliečių asmens tapatybės kortelių kontaktines elektronines laikmenas įrašomų elektroninių sertifikatų sudarymo, tvarkymo ir naudojimo reikalavimus.

2. Šių taisyklių unikalus identifikatorius yra 1.3.6.1.4.1.33621.2.2.2. Identifikatoriaus pirmoji dalis 1.3.6.1.4.1.33621 yra unikalus Asmens dokumentų išrašymo centro prie Lietuvos Respublikos vidaus reikalų ministerijos numeris IANA įmonių registre, toliau sekanti identifikatoriaus dalis 2.2 žymi konkretų įmonės dokumentą – šias taisykles, paskutinis identifikatoriaus skaičius 2 žymi dokumento versijos pirmąjį skaitmenį. Šio taisyklių dokumento versijos numeris yra 2.1.

3. Pagal šias taisykles sudaromų sertifikatų savininkais gali būti tik Lietuvos Respublikos piliečiai, kuriems yra išduota asmens tapatybės kortelė. Papildomus ribojimus nustato Lietuvos Respublikos civilinis kodeksas. Į sertifikatus įrašomus asmens duomenis nustato Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas.

4. Pagal šias taisykles yra sudaromi dviejų rūšių sertifikatai:

4.1. kvalifikuotas elektroninio parašo sertifikatas, skirtas kvalifikuotam elektroniniam parašui patvirtinti;

4.2. asmens atpažinimo elektroninėje erdvėje sertifikatas, skirtas asmens tapatybei elektroninėje erdvėje nustatyti.

5. Pagal šias taisykles sudaromuose sertifikatuose gali būti įrašomi tik tokie parašo patvirtinimo duomenys, kurie kartu su juos atitinkančiais parašo kūrimo duomenimis yra generuoti asmens tapatybės kortelės kontaktinėje elektroninėje laikmenoje, kuri yra kvalifikuotas elektroninio parašo kūrimo įtaisas.

6. Šiose taisyklėse vartojamos sąvokos:

6.1. **Kriptografinis modulis** – patikimumo užtikrinimo paslaugų teikėjo kriptografiniams raktams generuoti, apsaugoti bei elektroniniam parašui kurti naudojama techninė ir su ja susijusi programinė įranga.

6.2. **Kriptografinių raktų pora** – matematiškai susijusių privačiojo ir viešojo kriptografinių raktų pora.

6.3. **Negaliojančių sertifikatų sąrašas** – patikimumo užtikrinimo paslaugų teikėjo periodiškai leidžiamas sertifikatų, kurių galiojimas atšauktas ar laikinai sustabdytas, elektroninio formato sąrašas.

6.4. **Piliečio sertifikatai** – į Lietuvos Respublikos piliečių asmens tapatybės kortelių kontaktines elektronines laikmenas įrašomi kvalifikuoti elektroninio parašo sertifikatai ir asmens atpažinimo elektroninėje erdvėje sertifikatai.

6.5. **Privatusis kriptografinis raktas** – unikalūs elektroninio parašo kūrimo duomenys.

6.6. **Registravimo tarnyba** – patikimumo užtikrinimo paslaugų teikėjo arba kitos įgaliotos institucijos struktūrinis padalinys, priimantis piliečių prašymus išduoti sertifikatus, laikinai sustabdyti arba atšaukti išduotų sertifikatų galiojimą, panaikinti sertifikatų galiojimo laikiną sustabdymą bei atsakingas už šiuose prašymuose pateiktų duomenų patikrinimą ir prašymus teikiančių asmenų tapatybės nustatymą.

6.7. **Sertifikatais pasikliaujančios šalys** – fiziniai ir juridiniai asmenys, pasikliaujantys elektroniniais parašais, patvirtintais patikimumo užtikrinimo paslaugų teikėjo sudarytais sertifikatais.

6.8. **Sertifikato savininkas** – fizinis asmuo, kurio vardu sudaromas sertifikatas.

6.9. **Sertifikatų naudotojai** – sertifikatų savininkai ir sertifikatais pasikliaujančios šalys.

6.10. **Sertifikavimo paslaugos** – patikimumo užtikrinimo paslaugų teikėjo teikiamos sertifikatų sudarymo ir tvarkymo, taip pat informacijos apie sudarytų sertifikatų galiojimo statusą teikimo paslaugos.

6.11. **Sertifikavimo tarnyba** – aparatinė ir su ja susijusi programinė įranga, naudojama sertifikatams sudaryti ir tvarkyti.

6.12. **Viešasis kriptografinis raktas** – į sertifikatą įrašomi unikalūs elektroninio parašo patvirtinimo duomenys.

6.13. Kitos šiose taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (toliau – Reglamentas (ES) Nr. 910/2014).

7. Reikalavimus patikimumo užtikrinimo paslaugų teikėjams bei jų teikiamoms paslaugoms nustato Reglamentas (ES) Nr. 910/2014, Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas ir jų įgyvendinamieji teisės aktai. Sudarant ir tvarkant piliečio sertifikatus turi būti vadovaujamasi Europos telekomunikacijų standartų instituto standartais ETSI EN 319 401, ETSI EN 319 411-1 ir ETSI EN 319 411-2.

8. Šias taisykles administruojančio darbuotojo kontaktinė informacija yra pateikiama taisyklių priede.

II SKYRIUS
INFORMACIJOS SKELBIMAS

9. Patikimumo užtikrinimo paslaugų teikėjas savo interneto svetainėje turi skelbti taisykles, sertifikavimo veiklos nuostatus ir sertifikatų sudarymo bei tvarkymo sąlygas. Ši informacija turi būti viešai prieinama 7 dienas per savaitę, 24 valandas per parą.

10. Patikimumo užtikrinimo paslaugų teikėjas sertifikatų savininkų asmens duomenis privalo tvarkyti ir saugoti, vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo

tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB. Sudaryti sertifikatai ir juose įrašyti asmens duomenys viešai neskelbiami.

III SKYRIUS
ASMENŲ TAPATYBĖS NUSTATYMAS

11. Pirmą kartą išduodant piliečio sertifikatus, asmenų tapatybė nustatoma vadovaujantis Asmens tapatybės kortelės ir paso išdavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos vidaus reikalų ministro ir Lietuvos Respublikos užsienio reikalų ministro 2015 m. kovo 19 d. įsakymu Nr. 1V-200/V-62 „Dėl Asmens tapatybės kortelės ir paso išdavimo tvarkos aprašo patvirtinimo“.

12. Atnaujinant piliečio sertifikatus, taip pat teikiant prašymus atšaukti ar laikinai sustabdyti sertifikatų galiojimą ar panaikinti sertifikatų galiojimo laikiną sustabdymą, piliečio asmens tapatybė nustatoma vadovaujantis sertifikavimo veiklos nuostatais.

IV SKYRIUS
PILIEČIO SERTIFIKATŲ SUDARYMO IR TVARKYMO REIKALAVIMAI

Piliečių registravimas

13. Patikimumo užtikrinimo paslaugų teikėjas, vykdydamas asmenų registravimo sertifikatams gauti funkcijas, privalo:

13.1. užtikrinti registracijos duomenų konfidencialumą ir vientisumą;

13.2. užtikrinti registravimo tarnybų, su kuriomis registravimo procedūros metu keičiamasi duomenimis, identifikavimą.

Sertifikatų sudarymas

14. Sertifikatų sudarymo procesas ir sudaryti sertifikatai turi atitikti šiuos reikalavimus:

14.1. sudaromi kvalifikuoti elektroninio parašo sertifikatai turi atitikti Reglamente (ES) Nr. 910/2014 kvalifikuotiems elektroninio parašo sertifikatams nustatytus reikalavimus;

14.2. kriptografinių raktų poros turi būti generuojamos saugiai;

14.3. sertifikato sudarymo procedūra turi būti saugiai susieta su asmenų registravimo sertifikatams gauti procedūra;

14.4. sertifikato sudarymo procedūra turi būti saugiai susieta su kriptografinių raktų poros generavimo procedūra;

14.5. privačiųjų kriptografinių raktų slaptumas turi būti išlaikytas iki jų įteikimo sertifikatų savininkui;

14.6. kvalifikuoti elektroninio parašo kūrimo įtaisai sertifikatų savininkams turi būti perduoti saugiai;

14.7. kiekviename vienos ir tos pačios rūšies sertifikate nurodyti sertifikato savininko identifikavimo duomenys turi būti unikalūs tarp visų patikimumo užtikrinimo paslaugų teikėjo sudarytų sertifikatų.

15. Pasikeitus sertifikate įrašytiems sertifikato savininko duomenims arba sertifikate įrašytuose duomenyse pastebėjus klaidų, tokio sertifikato galiojimas turi būti atšaukiamas ir jo vietoje sudaromas naujas sertifikatas.

16. Išduodant naują sertifikatą visada turi būti sukuriami nauji elektroninio parašo kūrimo ir patvirtinimo duomenys.

17. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad:

17.1. jo sudaromi kriptografiniai raktai būtų sudaromi naudojant algoritmus, kurie atitinka kvalifikuoto elektroninio parašo saugumui keliamus reikalavimus visą juos atitinkančio sertifikato galiojimo laikotarpį;

17.2. jo sudaromų kriptografinių raktų ilgiai būtų tinkami naudojimui visą juos atitinkančio sertifikato galiojimo laikotarpį, atsižvelgiant į kvalifikuoto elektroninio parašo saugumui ir kūrimo algoritmams keliamus reikalavimus.

18. Kriptografinių raktų poroms generuoti ir saugoti turi būti naudojami Reglamento (ES) Nr. 910/2014 29 straipsnio reikalavimus atitinkantys kvalifikuoti elektroninio parašo kūrimo įtaisai.

Sertifikatų išdavimas

19. Patikimumo užtikrinimo paslaugų teikėjas, prieš sudarydamas sertifikatus, turi pateikti būsimam sertifikato savininkui sertifikatų sudarymo ir tvarkymo sąlygų dokumentą, kuris skirtas geriau susipažinti su pagrindiniais sertifikavimo veiklos aspektais, tačiau nekeičia ir nepavaduoja taisyklių ar sertifikavimo veiklos nuostatų.

20. Sertifikatų sudarymo ir tvarkymo sąlygų dokumente turi būti nurodyta:

20.1. patikimumo užtikrinimo paslaugų teikėjo pavadinimas ir kontaktai;

20.2. sertifikatų naudojimo apribojimai;

20.3. sertifikatų galiojimo tikrinimo, atšaukimo ir laikino sustabdymo procedūros;

20.4. sertifikatų sudarymo ir tvarkymo įrašų saugojimo laikotarpis;

20.5. sertifikatų savininko pareigos;

20.6. sertifikatais pasikliaujančių šalių pareigos;

20.7. patikimumo užtikrinimo paslaugų teikėjo pareigos ir atsakomybė;

20.8. informacija apie patikimumo užtikrinimo paslaugų teikėjo garantinius įsipareigojimus bei draudimo programas;

20.9. taikomų sutarčių, sertifikavimo veiklos nuostatų, taisyklių ir kitų susijusių dokumentų identifikacija ir nuorodos;

20.10. taikomų asmens duomenų apsaugos taisyklių aprašas ir nuorodos;

20.11. jei už teikiams paslaugas taikomi mokesčiai, taikomų piniginių lėšų sugrąžinimo taisyklių aprašas ir nuorodos;

20.12. taikomos teisės nustatymas, skundų procedūra, ginčų sprendimo mechanizmai;

20.13. informacija apie patikimumo užtikrinimo paslaugų teikėjo statusą;

20.14. jei buvo atliktas sertifikavimo veiklos atitikties Reglamento (ES) Nr. 910/2014 reikalavimams vertinimas, tai nurodoma atitikties vertinimo įstaiga ir vertinimo išvada.

21. Su sertifikato savininku turi būti sudarytas rašytinis susitarimas, kuriame sertifikato savininko parašu turi būti patvirtinta, kad jis susipažino ir sutinka su sertifikatų sudarymo ir tvarkymo sąlygomis.

22. Sudarytus sertifikatus jų savininkas turi atsiimti asmeniškai ir raštu patvirtinti sertifikatų, kvalifikuoto elektroninio parašo kūrimo įtaiso (asmens tapatybės kortelės) ir asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenų priėmimo faktą.

Parašo kūrimo ir patvirtinimo duomenų bei juos atitinkančių sertifikatų naudojimas

23. Sertifikato savininkas turi:

23.1. sertifikavimo veiklos nuostatų nustatyta tvarka teikti patikimumo užtikrinimo paslaugų teikėjui tikslią ir išsamią informaciją, reikalingą asmens tapatybei nustatyti ir sertifikatams sudaryti;

23.2. naudoti asmens tapatybės kortelėje esančius parašo kūrimo ir patvirtinimo duomenis bei juos atitinkančius sertifikatus tik 4 punkte nurodytiems tikslams, laikantis sertifikate nurodytų naudojimo apribojimų;

23.3. naudoti sertifikatus tik jų galiojimo laikotarpiu. Sertifikatų galiojimo laikotarpiu gavęs pranešimą ar kitaip sužinojęs, kad jam išduotų sertifikatų galiojimas yra atšauktas arba sertifikatus sudariusi sertifikavimo tarnyba tapo nepatikima, nedelsiant ir visam laikui nutraukti jam išduotus sertifikatus atitinkančių parašo kūrimo duomenų naudojimą;

23.4. pasirūpinti, kad parašo kūrimo duomenimis (asmens tapatybės kortele kaip pasirašymo elektroniniu parašu priemone) nepasinaudotų kiti asmenys;

23.5. sertifikatų galiojimo laikotarpiu praradęs parašo kūrimo duomenų (asmens tapatybės kortelės) kontrolę nedelsiant kreiptis į patikimumo užtikrinimo paslaugų teikėją su prašymu atšaukti juos atitinkančių sertifikatų galiojimą;

23.6. sertifikatų galiojimo laikotarpiu pasikeitus sertifikatuose įrašytiems duomenims arba pastebėjus, kad sertifikatuose yra įrašyti neteisingi duomenys, taip pat sužinojus, kad asmens tapatybės kortelės kontaktinės elektroninės laikmenos aktyvavimo duomenys (slaptažodis) galėjo tapti ar tapo žinomi kitiems asmenims, nedelsiant ir visam laikui nutraukti parašo kūrimo duomenų naudojimą bei kreiptis į patikimumo užtikrinimo paslaugų teikėją su prašymu atšaukti juos atitinkančių sertifikatų galiojimą;

23.7. leisti patikimumo užtikrinimo paslaugų teikėjui naudoti ir saugoti asmens duomenis, kaip to reikalauja taisyklės ir sertifikavimo veiklos nuostatai.

24. Sertifikatais pasikliaujančios šalys turi būti susipažinusios su taisyklėmis ir sertifikavimo veiklos nuostatais. Prieš spręsdamos apie sertifikato patikimumą, jos turi:

24.1. įsitikinti sertifikato galiojimu;

24.2. patikrinti visų sertifikatų seką sudarančių sertifikatų galiojimą;

24.3. įsitikinti, kad sertifikatas naudojamas pagal paskirtį, nurodytą sertifikate.

Sertifikatų galiojimo atšaukimas ir laikinas sustabdymas

25. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad sertifikatų galiojimo atšaukimas ir laikinas sustabdymas būtų vykdomi laiku, tinkamai patikrinus gautus įgaliotų asmenų prašymus.

26. Patikimumo užtikrinimo paslaugų teikėjo sertifikavimo veiklos nuostatuose turi būti nustatytos sertifikatų galiojimo atšaukimo ir laikino sustabdymo procedūros, kuriose turi būti nurodyta:

26.1. asmenys, kurie gali pateikti prašymą atšaukti ar laikinai sustabdyti sertifikato galiojimą;

26.2. prašymo pateikimo tvarka;

26.3. sertifikato galiojimo laikino sustabdymo ir galiojimo atšaukimo atvejai ir priežastys;

26.4. informacijos apie sertifikatų galiojimo statusą teikimo būdai.

27. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad:

27.1. gauti prašymai atšaukti ar laikinai sustabdyti sertifikato galiojimą būtų išnagrinėti nedelsiant;

27.2. prašymai atšaukti ar laikinai sustabdyti sertifikato galiojimą yra autentiški ir teisėti pagal sertifikavimo veiklos nuostatų reikalavimus;

27.3. maksimalus laikotarpis nuo prašymo atšaukti ar laikinai sustabdyti sertifikato galiojimą gavimo iki informacijos apie naują sertifikato galiojimo statusą pateikimo būtų ne ilgesnis kaip 24 valandos;

27.4. maksimalus laikotarpis nuo sprendimo atšaukti ar laikinai sustabdyti sertifikato galiojimą iki informacijos apie naują sertifikato galiojimo statusą pateikimo būtų ne ilgesnis nei 60 minučių;

27.5. sertifikato galiojimo atšaukimas negalėtų būti panaikintas;

27.6. sertifikatų galiojimo statuso pasikeitimus registruojančių sistemų laikas būtų sinchronizuojamas su pasauliniu koordinuotuoju laiku ne rečiau kaip kartą per 24 valandas.

28. Sertifikato galiojimo atšaukimas ir laikinas sustabdymas negali būti vykdomi atgaline data ar laiku.

Informacijos apie sertifikatų galiojimo statusą teikimas

29. Informaciją apie sertifikato galiojimo statusą patikimumo užtikrinimo paslaugų teikėjas turi teikti per užklausų sistemą teikdamas atsakymus apie sertifikato galiojimo statusą sertifikato galiojimo tikrinimo metu (OCSP).

30. Informacija apie sertifikato galiojimo statusą turi būti teikiama 7 dienas per savaitę, 24 valandas per parą. Jei dėl tiesiogiai nuo patikimumo užtikrinimo paslaugų teikėjo nepriklausančių priežasčių sutrinka informacijos apie sertifikato galiojimo statusą teikimas, patikimumo užtikrinimo paslaugų teikėjas turi imtis visų įmanomų priemonių jam atstatyti per laiką, nustatytą šias taisykles įgyvendinančiuose sertifikavimo veiklos nuostatuose.

31. Informacija apie sertifikato galiojimo statusą turi būti teikiama taip pat ir pasibaigus sertifikato galiojimo laikotarpiui.

32. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti jo teikiamos informacijos apie sertifikato galiojimo statusą vientisumą ir autentiškumą. Ši informacija turi būti vieša ir prieinama tarptautiniu mastu.

V SKYRIUS
ĮRANGOS, VALDYMO IR PRODEDŪRŲ KONTROLĖ

Bendrosios nuostatos

33. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad jo vykdoma sertifikavimo veikla atitiktų informacijos saugos valdymui keliamus įstatymų ir kitų teisės aktų reikalavimus.

34. Patikimumo užtikrinimo paslaugų teikėjas privalo:

34.1. apibrėžti ir įgyvendinti informacijos saugos politiką, kuri turi būti dokumentuota, patvirtinta vadovybės, reguliariai peržiūrima ir pagal poreikį atnaujinama;

34.2. skleisti informacijos saugos politiką savo ir kitų sertifikavimo paslaugų teikimo procese dalyvaujančių institucijų darbuotojams;

34.3. kai tai yra taikytina, informuoti apie informacijos saugos politikos pasikeitimus trečiąsias šalis – sertifikatų naudotojus, atitikties vertinimo įstaigą, priežiūros įstaigą ar kitas priežiūros institucijas;

34.4. užtikrinti, kad būtų apibrėžtos, įgyvendinamos, prižiūrimos ir dokumentuojamos visos su patikimumo užtikrinimo paslaugų teikėjo įrenginiais, sistemomis ir informaciniu turtu susijusios saugumo valdymo priemonės ir procedūros;

34.5. periodiškai atlikti saugumo ir veiklos procedūrų reikalavimams nustatyti būtiną rizikos analizę;

34.6. inventorizuoti sertifikavimo paslaugų teikimui naudojamą ir paslaugų teikimo procese sukauptą informacinį turtą ir pagal rizikos analizės rezultatus suklasifikuoti šio turto saugos reikalavimus;

34.7. užtikrinti, kad visi įtakos informacijos saugai turintys pakeitimai būtų patvirtinti patikimumo užtikrinimo paslaugų teikėjo vadovybės;

34.8. užtikrinti, kad sertifikavimo paslaugoms teikti naudojamų sistemų konfigūracija būtų reguliariai tikrinama, siekiant nustatyti galimas neatitiktis informacijos saugos politikos reikalavimams;

34.9. užtikrinti, kad informacijos kaupikliai ir laikmenos, kuriose saugoma jautri informacija, būtų sunaikinti iš karto po to, kai jie tampa nereikalingi sertifikavimo veiklai vykdyti.

Fizinio saugumo kontrolė

35. Patikimumo užtikrinimo paslaugų teikėjas turi kontroliuoti fizinę prieigą prie sistemų, kurios yra kritinės paslaugų teikimui, ir sumažinti fizinio pažeidimo riziką iki priimtino lygio.

36. Patikimumo užtikrinimo paslaugų teikėjas turi:

36.1. laikyti sertifikatų sudarymo, kvalifikuotų elektroninio parašo kūrimo įtaisų rengimo ir sertifikatų galiojimo atšaukimo ar laikino sustabdymo įrangą fiziškai atskirtose zonose, į kurias patekti galėtų tik tam teisę turintys asmenys. Bet kokios bendrai su kitomis organizacijomis naudojamos patalpos turi būti už šių zonų ribų;

36.2. užtikrinti, kad zonos, kuriose laikoma sertifikatų sudarymo, kvalifikuotų elektroninio parašo kūrimo įtaisų rengimo ir sertifikatų galiojimo atšaukimo ar laikino sustabdymo įranga, būtų stebimos, teisės į šias zonas patekti neturintys asmenys į jas patekti galėtų tik lydimi tam teisę turinčių asmenų ir kiekvienas patekimas į šias zonas būtų registruojamas;

36.3. įgyvendinti priemones, skirtas užtikrinti turto apsaugą nuo praradimo, sugadinimo, neleistino naudojimo ir apsaugoti nuo veiklos sustabdymo;

36.4. įgyvendinti priemones, skirtas užtikrinti informacijos ir informacijos apdorojimo priemonių apsaugą nuo neleistino naudojimo ar vagystės;

36.5. įgyvendinti priemones, skirtas apsaugoti su paslaugų teikimu susijusią aparatinę ir programinę įrangą, informaciją bei jos kaupiklius nuo nesankcionuoto paėmimo iš nustatytos jų laikymo vietos.

37. Patikimumo užtikrinimo paslaugų teikėjas turi įgyvendinti šias patalpų, kuriose laikoma paslaugų teikimui naudojama įranga, fizinės apsaugos ir apsaugos nuo aplinkos poveikio priemones:

37.1. fizinės prieigos kontrolę;

37.2. priešgaisrinę apsaugą;

37.3. apsaugą nuo komunalinių paslaugų (pvz., elektros energijos, telekomunikacijų) teikimo sutrikimų;

37.4. apsaugą nuo patalpų užliejimo;

37.5. apsaugą nuo įsilaužimo ir vagysčių.

Procedūrų saugumo kontrolė

38. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad loginė prieiga prie paslaugų teikimui naudojamų sistemų būtų suteikta tik tinkamai autorizuotam personalui:

38.1. sertifikavimo paslaugų teikimui naudojamų sistemų administratorių, auditorių ir operatorių prieigos teisės turi būti valdomos;

38.2. sertifikavimo paslaugų teikimui naudojamose sistemose turi būti įmanoma atskirti aukštos atsakomybės pareigybių teises. Pagalbinių programų naudojimas turi būti ribojamas ir kontroliuojamas;

38.3. sertifikatų sudarymo ir tvarkymo kritines operacijas atliekantys darbuotojai turi būti identifikuojami ir autentifikuojami;

38.4. patikimumo užtikrinimo paslaugų teikėjo darbuotojų veiksmai turi būti kontroliuojami, fiksuojant ir išsaugant informaciją apie sistemų naudojimą.

Personalo patikimumo kontrolė

39. Patikimumo užtikrinimo paslaugų teikėjo darbuotojai turi turėti aukštąjį išsilavinimą bei žinių, patirties ir kvalifikaciją, kurių reikia sertifikavimo paslaugoms teikti.

40. Darbuotojams, pažeidusiems patikimumo užtikrinimo paslaugų teikėjo informacijos saugos politikos ir procedūrų reikalavimus, turi būti taikomos tinkamos drausminės nuobaudos.

41. Patikimumo užtikrinimo paslaugų teikėjo informacijos saugos politikoje nustatytos už saugą atsakingų darbuotojų pareigos ir atsakomybės turi būti nurodytos šių darbuotojų pareigybių aprašymuose. Aukštos atsakomybės pareigybės, nuo kurių tiesiogiai priklauso patikimumo užtikrinimo paslaugų teikėjo veiklos saugumas, turi būti aiškiai apibrėžtos.

42. Visų su sertifikavimo paslaugų teikimu susijusių patikimumo užtikrinimo paslaugų teikėjo darbuotojų pareigybių aprašymai turi būti parengti atsižvelgiant į konkrečios pareigybės paskirtį ir vadovaujantis funkcijų atskyrimo ir mažiausios prieigos teisės principais. Kiekvienai pareigybei turi būti priskirtas atitinkamas atsakomybės lygis, kuris nustatomas atsižvelgiant į tai pareigybei priskirtas funkcijas ir joms atlikti būtinas prieigos teises. Atsižvelgiant į pareigybės paskirtį ir funkcijas, kiekvienos pareigybės aprašyme nustatomi pareigybei užimti reikalingi įgūdžių ir patirties reikalavimai.

43. Vadovaujančias pareigas einantys darbuotojai turi išmanyti elektroninio parašo technologijas ir turėti informacijos saugos ir rizikos valdymo patirties.

44. Aukštos atsakomybės pareigas einantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai negali turėti jokių interesų, kurie galėtų turėti įtakos patikimumo užtikrinimo paslaugų teikėjo veiklos nešališkumui.

45. Patikimumo užtikrinimo paslaugų teikėjas turi nustatyti šias aukštos atsakomybės pareigas ir joms priskirti tokią atsakomybę:

45.1. Sertifikatų valdymo informacinės sistemos saugos įgaliotinis – atsakingas už sistemos elektroninės informacijos saugos politikos įgyvendinimo koordinavimą ir priežiūrą;

45.2. sertifikavimo tarnybos pareigūnas – atsakingas už sertifikavimo paslaugų teikimui reikalingų infrastruktūros sertifikatų išdavimą, patikimumo užtikrinimo paslaugų teikėjo valdomų sertifikatų sudarymo ir tvarkymo operacijų tvirtinimą;

45.3. sertifikavimo tarnybos administratorius – atsakingas už patikimumo užtikrinimo paslaugų teikėjo sertifikatų sudarymui ir tvarkymui naudojamų sertifikavimo tarnybų diegimą, konfigūravimą ir palaikymą;

45.4. sertifikavimo tarnybos operatorius – atsakingas už sertifikatų sudarymo ir tvarkymo sistemų nenutrūkstamą veikimą, įgaliotas daryti atsargines kopijas ir vykdyti informacijos iš jų atstatymo procedūras;

45.5. sertifikavimo tarnybos auditorius – atsakingas už patikimumo užtikrinimo paslaugų teikėjo patikimų sistemų archyvų ir audito įrašų peržiūrą, perkėlimą į archyvus ir nereikalingų įrašų išvalymą.

46. Patikimumo užtikrinimo paslaugų teikėjas negali priimti dirbti asmens, kuris įstatymų nustatyta tvarka pripažintas kaltu dėl nusikalstamos veikos vykdymo ir turi neišnykusį ar nepanaikintą teistumą.

Įrašų kaupimas ir archyvavimas

47. Patikimumo užtikrinimo paslaugų teikėjas, siekdamas pateikti tinkamos sertifikavimo veiklos įrodymus teisminiuose procesuose bei užtikrinti šios veiklos tęstinumą, privalo kaupti įrašus

apie visas sertifikatų sudarymo ir tvarkymo operacijas. Kaupdamas įrašus, patikimumo užtikrinimo paslaugų teikėjas privalo:

47.1. užtikrinti einamųjų ir archyvinių įrašų konfidencialumą ir vientisumą;

47.2. užtikrinti, kad įrašai būtų saugomi sertifikavimo veiklos nuostatuose nustatyta tvarka;

47.3. užtikrinti, kad būtų fiksuojamas tikslus visų reikšmingų su patikimumo užtikrinimo paslaugų teikėjo veikla, kriptografinių raktų tvarkymu ir sertifikavimo paslaugų teikimui naudojamų sistemų laiko sinchronizavimu susijusių įvykių laikas;

47.4. užtikrinti, kad sertifikatų sudarymo ir tvarkymo operacijų įrašų saugojimo terminas būtų nustatytas atsižvelgiant į laikotarpį, per kurį patikimumo užtikrinimo paslaugų teikėjas teisminių procesų atveju turi teikti tinkamai vykdytos sertifikavimo veiklos įrodymus;

47.5. fiksuojamus įvykių duomenis apsaugoti nuo pakeitimo ar sunaikinimo visą jų saugojimo laikotarpį;

47.6. registruoti visus saugos incidentus bei neeilinius veiklos įvykius.

48. Patikimumo užtikrinimo paslaugų teikėjas privalo kaupti asmenų registravimo sertifikatams gauti informaciją, įskaitant prašymus sudaryti ar atnaujinti sertifikatus.

49. Patikimumo užtikrinimo paslaugų teikėjas privalo užtikrinti, kad būtų kaupiama ši asmenų registravimo sertifikatams gauti informacija:

49.1. prašymuose sudaryti sertifikatus pateiktų dokumentų identifikavimo duomenys;

49.2. prašymą priėmusio darbuotojo identifikavimo duomenys;

49.3. prašymą priėmusios registravimo tarnybos pavadinimas.

50. Patikimumo užtikrinimo paslaugų teikėjas privalo registruoti:

50.1. visus patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų gyvavimo ciklo įvykius;

50.2. visus sudaromų sertifikatų gyvavimo ciklo įvykius;

50.3. visus asmenims generuojamų kriptografinių raktų gyvavimo ciklo įvykius;

50.4. visus įvykius, susijusius su kvalifikuotų elektroninio parašo kūrimo įtaisų parengimu;

50.5. visus įvykius, susijusius su sertifikatų galiojimo statuso keitimu, įskaitant prašymus, pranešimus ir su jų vykdymu susijusius veiksmus.

51. Asmenų registravimo sertifikatams gauti metu surinkta informacija ir informacija apie patikimumo užtikrinimo paslaugų teikėjo generuojamų kriptografinių raktų gyvavimo ciklo įvykius turi būti saugoma ne mažiau kaip 7 metus nuo išduotų sertifikatų galiojimo pabaigos.

Veiklos atkūrimas didelių incidentų ir paslaugų patikimumo praradimo atveju

52. Siekiant riboti galimų informacijos saugos incidentų poveikį, patikimumo užtikrinimo paslaugų teikėjas turi nuolatos stebėti sertifikavimo paslaugų teikimui naudojamas informacines sistemas. Stebėjimas turi būti nuolatinis arba atliekamas automatiniu būdu reguliariai peržiūrint sistemų audito žurnalus ir signalizuojant apie kritinius saugumo įvykius.

53. Turi būti stebimi sistemų audito funkcijų paleidimo ir stabdymo įvykiai, paslaugų pasiekiamumas ir naudojimo intensyvumas.

54. Pastebėjus neįprastą sistemų veikimą ar gavus automatinį perspėjimą, turi būti reaguojama nedelsiant.

55. Jeigu informacijos saugos pažeidimas ar duomenų vientisumo praradimas gali turėti neigiamą poveikį sertifikatų naudotojams, pastarieji apie informacijos saugos pažeidimą ar duomenų vientisumo praradimą turi būti informuojami nedelsiant.

56. Sistemų veikimo sutrikimų padariniai turi būti minimizuoti naudojant pranešimų apie incidentus ir reagavimo į juos procedūras.

57. Patikimumo užtikrinimo paslaugų teikėjas turi nedelsdamas ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo to momento, kai sužino apie bet kokį informacijos saugos pažeidimą ar duomenų vientisumo praradimą, kuris gali turėti reikšmingą poveikį teikiamoms paslaugoms ar tvarkomų asmens duomenų saugumui, apie tai pranešti priežiūros įstaigai ir kitoms suinteresuotoms šalims.

58. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad bet kokių informacijos saugos incidentų atveju, tarp jų ir patikimumo užtikrinimo paslaugų teikėjo privačiųjų kriptografinių raktų kontrolės praradimo atveju, nedelsiant būtų imtasi visų galimų priemonių kaip įmanoma sumažinti incidento pasekmes ir kuo greičiau atkurti normalią veiklą. Dideliems incidentams valdyti patikimumo užtikrinimo paslaugų teikėjas turi parengti ir reguliariai atnaujinti veiklos tęstinumo valdymo planą.

59. Patikimumo užtikrinimo paslaugų teikėjas turi reguliariai daryti esminės informacijos ir programinės įrangos atsargines kopijas. Esminės informacijos ir programinės įrangos atstatymui iš atsarginių kopijų turi būti parengta tinkama įranga, užtikrinanti visišką esminės informacijos ir programinės įrangos atstatymą.

60. Privačiojo kriptografinio rakto kontrolės praradimo atveju, patikimumo užtikrinimo paslaugų teikėjas turi nedelsiant imtis šių minimalių veiksmų:

60.1. informuoti visus sertifikatų naudotojus ir kitus su patikimumo užtikrinimo paslaugų teikėjo veikla susijusius asmenis;

60.2. nurodyti, kad nebekontroliuojamu privačiuoju kriptografiniu raktu pasirašyti sertifikatai, per užklausų sistemą išsiųsti pranešimai apie sertifikatų galiojimo statusą ir negaliojančių sertifikatų sąrašai negali būti laikomi patikimais;

60.3. nutraukti nebekontroliuojamu privačiuoju kriptografiniu raktu pasirašytų sertifikatų galiojimą.

61. Paaiškėjus, kad kuris nors iš patikimumo užtikrinimo paslaugų teikėjo sertifikavimo paslaugų teikimui naudojamų kriptografinių algoritmų tapo nepatikimu, patikimumo užtikrinimo paslaugų teikėjas privalo nedelsiant apie tai informuoti visus sertifikatų naudotojus ir kitus su patikimumo užtikrinimo paslaugų teikėjo veikla susijusius asmenis bei sudaryti sertifikatų, kuriems sudaryti buvo naudojamas nepatikimu tapęs algoritmas, galiojimo nutraukimo planą.

Sertifikavimo paslaugų teikimo nutraukimas

62. Patikimumo užtikrinimo paslaugų teikėjas turi turėti sertifikavimo paslaugų teikimo veiklos nutraukimo planą, kuriame turi būti nurodyti:

62.1. sertifikatų naudotojų informavimo būdai;

62.2. patikimumo užtikrinimo paslaugų teikėjo įsipareigojimų perdavimo apimtis ir sąlygos.

63. Prieš nutraukdamas sertifikavimo paslaugų teikimą, patikimumo užtikrinimo paslaugų teikėjas turi:

63.1. ne vėliau kaip prieš tris mėnesius iki veiklos nutraukimo dienos apie tai informuoti visus sertifikatų naudotojus ir priežiūros įstaigą;

63.2. nutraukti visų trečiųjų šalių įgaliojimus veikti patikimumo užtikrinimo paslaugų teikėjo vardu teikiant sertifikavimo paslaugas;

63.3. perduoti savo įsipareigojimus patikimai šaliai, esant galimybei, perduoti sertifikavimo paslaugų teikimą kitam patikimumo užtikrinimo paslaugų teikėjui;

63.4. sunaikinti paslaugų teikimui naudotus privačiuosius raktus, įskaitant jų atsargines kopijas.

64. Nutraukęs sertifikavimo paslaugų teikimą, patikimumo užtikrinimo paslaugų teikėjas turi protingą laikotarpį teikti sertifikatais pasikliaujančioms šalims paslaugų teikimui naudotų sertifikavimo tarnybų viešojo rakto sertifikatus arba perduoti šią pareigą vykdyti patikimai šaliai.

VI SKYRIUS
TECHNINĖS SAUGUMO PRIEMONĖS

Patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų sudarymas ir tvarkymas

65. Patikimumo užtikrinimo paslaugų teikėjo privačiųjų kriptografinių raktų saugumui užtikrinti turi būti naudojamos tokios techninės priemonės ir procedūros, kurios užtikrintų tinkamą privačiojo kriptografinio rakto apsaugą nuo neteisėto atskleidimo ar naudojimo, garantuotų privataus kriptografinio rakto konfidencialumą ir vientisumą.

66. Patikimumo užtikrinimo paslaugų teikėjo kriptografiniai raktai turi būti sudaromi fiziškai saugioje aplinkoje. Raktų sudarymo procedūroje privalo dalyvauti ne mažiau kaip du aukštos atsakomybės pareigas einantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai, tarp kurių privalo būti sertifikavimo tarnybos pareigūnas.

67. Raktų sudarymo procedūra turi būti patvirtinta protokolu, kurį turi pasirašyti visi procedūros dalyviai. Šakninės sertifikavimo tarnybos raktų generavimo atveju protokolą turi pasirašyti patikimas nepriklausomas asmuo.

68. Patikimumo užtikrinimo paslaugų teikėjo kriptografiniams raktams sudaryti turi būti naudojama įranga, atitinkanti:

68.1. JAV Nacionalinio standartų ir technologijų instituto standarto FIPS PUB 140-2 „Saugos reikalavimai kriptografiniams moduliams“ ne žemesnio kaip trečiojo saugumo lygmens (Level 3) reikalavimus arba;

68.2. Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ nustatytą informacinių technologijų saugumo įvertinimo užtikrinimo lygį EAL 4 atitinkančio apsaugos profilio reikalavimus.

69. Patikimumo užtikrinimo paslaugų teikėjo kriptografinių raktų ilgis ir generavimo algoritmas turi atitikti standarto ETSI TS 119 312 reikalavimus.

70. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad jo kriptografiniai raktai ir viešuosius raktus patvirtinantys sertifikatai būtų atnaujinami laiku, o sertifikatų naudotojai bei kitos suinteresuotos šalys apie atnaujinimą būtų informuojami taip, kad atnaujinimas nesukeltų jiems jokių nepatogumų ar nesutrikdytų jų veiklos.

71. Patikimumo užtikrinimo paslaugų teikėjas turi pateikti savo viešuosius kriptografinius raktus sertifikatais pasikliaujančioms šalims, užtikrindamas jų vientisumą ir kilmės autentiškumą.

72. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad jo privatūs kriptografiniai raktai būtų laikomi ir naudojami tik kartu su įranga, kuri atitinka šių taisyklių 68 punkto reikalavimus.

73. Jei patikimumo užtikrinimo paslaugų teikėjo privatieji kriptografiniai raktai ar jų kopijos laikomi ne kriptografiniame modulyje, jie turi būti šifruojami. Šifravimui turi būti naudojami tokie algoritmai ir parametrai, kurie užtikrintų privačiųjų kriptografinių raktų saugumą visą privačiųjų kriptografinių raktų numatytą naudojimo laikotarpį.

74. Patikimumo užtikrinimo paslaugų teikėjo privačiųjų kriptografinių raktų atsarginės kopijos turi būti daromos ir saugomos bei privatieji kriptografiniai raktai iš jų atstatomi tik saugioje aplinkoje. Raktų atsarginių kopijų darymo ir raktų atstatymo iš atsarginių kopijų procedūrose privalo dalyvauti ne mažiau kaip du aukštos atsakomybės pareigas einantys patikimumo užtikrinimo paslaugų teikėjo darbuotojai.

75. Patikimumo užtikrinimo paslaugų teikėjo privačiųjų kriptografinių raktų atsarginių kopijų apsaugos lygis turi būti lygiavertis kriptografinių raktų apsaugos lygiui ar už jį aukštesnis.

76. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti tinkamą jo privačiųjų kriptografinių raktų naudojimą, įskaitant bet neapsiribojant tuo, kad:

76.1. privatieji kriptografiniai raktai būtų naudojami tik pagal jų paskirtį;

76.2. privatieji kriptografiniai raktai būtų naudojami tik fiziškai saugioje aplinkoje;

76.3. visos privačiųjų kriptografinių raktų kopijos pasibaigus atitinkamų raktų numatytam naudojimo terminui būtų sunaikintos.

77. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad jo naudojami kriptografiniai moduliai nebuvo pažeisti iki jų pateikimo patikimumo užtikrinimo paslaugų teikėjui, taip pat jų sandėliavimo metu.

78. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad jo naudojami kriptografiniai moduliai veikia tinkamai.

79. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad nutraukus kriptografinių modulių naudojimą, juose esantys kriptografiniai raktai būtų sunaikinti.

Prieigos valdymas

80. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad prieiga prie paslaugų teikimui naudojamose sistemose tvarkomos informacijos būtų suteikta tik tinkamai autorizuotam personalui:

80.1. paslaugų teikimui naudojamos sistemos turi būti apsaugotos ugniasienėmis;

80.2. vietinio tinklo įranga turi būti laikoma saugioje aplinkoje;

80.3. sertifikatų sudarymo, jų galiojimo atšaukimo ir laikino sustabdymo sistemose turi būti naudojama nuolatinio stebėjimo ir signalizavimo sistema, skirta nustatyti ir registruoti neteisėtus bandymus prieiti prie sistemos išteklių bei juos užkirsti;

80.4. konfidencialūs duomenys turi būti apsaugoti nuo jų atskleidimo dėl antrinio laikmenų panaudojimo.

Sistemų veikimo užtikrinimas

81. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti, kad paslaugų teikimui naudojamos sistemos veiktų saugiai ir patikimai, o pokyčių sukeltų sutrikimų rizika būtų minimali:

81.1. įgyvendinant bet kokį sistemų plėtros projektą, projektavimo ir poreikių nustatymo etape turi būti atliekama saugumo reikalavimų analizė;

81.2. programinės įrangos atnaujinimas, modifikavimas ar skubus taisymas turi būti valdomas, dokumentuojant atliktus pakeitimus;

81.3. patikimumo užtikrinimo paslaugų teikėjo įrangos ir jo valdomos informacijos vientisumas turi būti apsaugotas nuo pažeidimų, kuriuos gali sukelti kompiuteriniai virusai, kenkėjiška programinė įranga ar neleistinos programinės įrangos naudojimas;

81.4. patikimumo užtikrinimo paslaugų teikėjo sistemose naudojami informacijos kaupikliai ir laikmenos turi būti tvarkomi saugiai, užtikrinant jų apsaugą nuo sugadinimo, vagystės, neteisėto panaudojimo ar susidėvėjimo;

81.5. patikimumo užtikrinimo paslaugų teikėjo sistemose naudojami informacijos kaupikliai ir laikmenos turi būti apsaugoti nuo susidėvėjimo visą juose esančių įrašų privalomojo saugojimo laikotarpį;

81.6. visų aukštos atsakomybės pareigas einančių darbuotojų vykdomos procedūros turi būti tiksliai apibrėžtos ir jų turi būti laikomasi;

81.7. saugumo spragoms užtaisyti skirti programinės įrangos atnaujinimai turi būti diegiami laiku, nebent jų diegimas galėtų pakenkti sistemų darbui;

81.8. ateityje reikalingų išteklių poreikis turi būti planuojamas.

Tinklo saugumo valdymas

82. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti sertifikavimo paslaugų teikimui naudojamų sistemų apsaugą nuo tinklo atakų:

82.1. patikimumo užtikrinimo paslaugų teikėjo vidinis kompiuterių tinklas turi būti padalintas į atskiras zonas, atsižvelgiant į jose esančių įrangos komponentų saugos ir atliekamų funkcijų reikalavimus;

82.2. prieiga prie zonų ir tarpusavio ryšiai turi būti ribojami taip, kad zonos būtų pasiekiamos tik su sertifikavimo paslaugų teikimu susijusioms funkcijoms vykdyti;

82.3. sertifikavimo paslaugų teikimui naudojamos sistemos turi būti administruojamos iš atskiro, tam skirto potinklio;

82.4. ryšių tarp atskirų sertifikavimo paslaugų teikimui naudojamų sistemų saugumui užtikrinti turi būti naudojamas šifravimas ir patikimas ryšio mazgų identifikavimas;

82.5. viešieji ir privatūs sertifikavimo paslaugų teikimui naudojamo tinklo adresai turi būti periodiškai skenuojami, siekiant nustatyti galimus pažeidžiamumus. Skenavimą turi atlikti kompetetingas ir nepriklausomas asmuo ar įstaiga;

82.6. sertifikavimo paslaugų teikimui naudojamoms sistemoms turi būti atliktas etiško įsilaužimo testas, kurį turi atlikti kompetetingas ir nepriklausomas asmuo ar įstaiga. Testas turi būti atliekamas pradedant sistemų naudojimą, taip pat atlikus ženklius sistemų pakeitimus.

VII SKYRIUS
KITOS NUOSTATOS

83. Patikimumo užtikrinimo paslaugų teikėjas gali nustatyti mokesčius už tam tikras sertifikavimo paslaugas, išskyrus mokestį už informacijos, reikalingos jo sudarytų sertifikatų patikimumui nustatyti, bei informacijos apie jo sudarytų sertifikatų galiojimo statusą teikimą.

84. Sertifikavimo paslaugos turi būti teikiamos vadovaujantis Lietuvos Respublikos įstatymais ir kitais teisės aktais, sudarant paslaugų vartotojams galimybes įsitikinti vykdomos veiklos legalumu.

85. Patikimumo užtikrinimo paslaugų teikėjas turi užtikrinti jo vykdomos veiklos patikimumą šiomis priemonėmis:

85.1. sertifikavimo paslaugos turi būti teikiamos vadovaujantis nediskriminavimo principu;

85.2. sertifikavimo paslaugos turi būti teikiamos jų vartotojams, kurie sutinka su sertifikatų sudarymo ir tvarkymo sąlygomis;

85.3. turi būti užtikrintas prievolių dėl atsakomybės už vykdomą sertifikavimo veiklą įvykdymas;

85.4. turi būti užtikrintas finansinis stabilumas ir ištekliai, reikalingi tinkamai įgyvendinti taisyklių reikalavimus;

85.5. turi būti nustatytos su sertifikavimo paslaugų teikimu susijusių ginčų sprendimo procedūros;

85.6. subrangos, samdos ir kitos veiklos funkcijų perdavimo sutartys turi būti tinkamai įformintos ir teisiškai galiojančios.

86. Patikimumo užtikrinimo paslaugų teikėjo vykdoma sertifikatų sudarymo, jų galiojimo atšaukimo ir laikino sustabdymo veikla turi būti nepriklausoma. Patikimumo užtikrinimo paslaugų teikėjo vadovai ir aukštos atsakomybės pareigas einantys darbuotojai negali turėti jokių interesų, kurie galėtų daryti neigiamą poveikį sertifikavimo veiklos patikimumui.

87. Veiklos nešališkumui užtikrinti, visa patikimumo užtikrinimo paslaugų teikėjo vykdoma sertifikatų sudarymo, jų galiojimo atšaukimo ir laikino sustabdymo veikla turi būti dokumentuota.

VIII SKYRIUS
TAISYKLIŲ ADMINISTRAVIMAS

88. Sertifikatų naudotojai turi vadovautis taisyklių, kurių unikalus identifikatorius įrašytas sertifikate, redakcija. Patvirtinus naują taisyklių redakciją, ji nedelsiant skelbiama patikimumo užtikrinimo paslaugų teikėjo tinklalapyje.

89. Taisyklės gali būti keičiamos pastebėjus jose klaidas ar atsiradus poreikiui jas atnaujinti.

90. Taisyklių pakeitimai gali būti:

90.1. esminiai, apie kuriuos turi būti pranešama sertifikatų naudotojams;

90.2. neesminiai, apie kuriuos sertifikatų naudotojams pranešti nėra privaloma.

91. Neesminiais pakeitimais laikomi rekomendacinio, paaiškinamojo, tikslinamojo pobūdžio informacijos arba už taisyklių tvarkymą atsakingų asmenų kontaktinių duomenų pakeitimai. Kitais atvejais pakeitimai yra esminiai. Visais atvejais, kai taisyklių pakeitimai yra susiję su sertifikavimo paslaugų saugumo lygio keitimu, taisyklių pakeitimai yra esminiai.

92. Atlikus esminius pakeitimus, keičiamas unikalus taisyklių identifikatorius (taisyklių dokumento versiją atitinkantis identifikatoriaus elementas – paskutinis identifikatoriaus skaitmuo) bei naujos taisyklių redakcijos dokumento versijos pirmas skaitmuo. Atlikus neesminius pakeitimus, taisyklių unikalus identifikatorius nėra keičiamas, o keičiamas tik naujos taisyklių redakcijos dokumento versijos antrasis skaitmuo.

93. Taisyklių peržiūra, keitimas ir tvirtinimas vykdomi tokia tvarka:

93.1. taisyklių pakeitimus gali inicijuoti patikimumo užtikrinimo paslaugų teikėjas arba sertifikatų naudotojai;

93.2. už informacijos saugos politiką atsakingi patikimumo užtikrinimo paslaugų teikėjo darbuotojai:

93.2.1. per vienerius metus nuo vėliausios taisyklių redakcijos paskelbimo peržiūri ir įsitikinta taisyklių aktualumu;

93.2.2. peržiūros metu nustačius poreikį keisti taisykles, inicijuoja taisyklių keitimą ir rengia naują taisyklių redakciją;

93.2.3. priima sprendimą teikti tvirtinti naują taisyklių redakciją.

93.3. esminių pakeitimų atveju, parengtas naujos taisyklių redakcijos projektas turi būti teikiamas suinteresuotoms šalims pastaboms ir pasiūlymams, paskelbiant projektą internete ne trumpesniam kaip 30 kalendorinių dienų laikotarpiui. Atsižvelgus į per 30 dienų gautas pastabas arba per šį laikotarpį negavus pastabų, taisyklių nauja redakcija teikiama tvirtinti;

93.4. neesminių pakeitimų atveju, nauja taisyklių redakcija teikiama tvirtinti iš karto ją parengus;

93.5. naują taisyklių redakciją tvirtina patikimumo užtikrinimo paslaugų teikėjo vadovas.

94. Apie naują taisyklių redakciją informuojama priežiūros įstaiga.

____

Piliečio sertifikato taisyklių priedas

TAISYKLES ADMINISTRUOJANČIO DARBUOTOJO KONTAKTINĖ INFORMACIJA

Įstaiga	Asmens dokumentų išrašymo centras prie Lietuvos Respublikos vidaus reikalų ministerijos
Asmuo	Nerijus Rudaitis
Adresas	Žirmūnų g. 1D, LT-09239 Vilnius
Tel.	(8 5) 271 8000
Faks.	(8 5) 271 8045
URL:	https://www.nsc.vrm.lt/
El.paštas:	nerijus.rudaitis@vrm.lt